

AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

- 1 1. (Currently Amended) A method for communicating cryptographic
2 data through multiple network layers, comprising:
3 receiving the cryptographic data at a node;
4 dividing the cryptographic data into multiple pieces; and
5 simultaneously encapsulating different pieces of the cryptographic data in
6 fields associated with different network layers of a protocol stack in a data packet,
7 wherein the cryptographic data is larger than a single field, and wherein the
8 cryptographic data is encapsulated within multiple fields associated with different
9 network layers of the protocol stack;
10 wherein the multiple fields ~~need to be~~are received simultaneously by a
11 receiving node ~~to~~that reconstructs an identity associated with the cryptographic
12 data; and
13 wherein the multiple fields ~~need to be~~are encapsulated simultaneously into
14 the data packet to ensure that the data packet can be routed through a network to
15 reach the receiving node.

- 1 2. (Original) The method of claim 1, wherein receiving the
2 cryptographic data involves performing at least one non-reversible function on a
3 piece of input data to produce the cryptographic data.

1 3. (Original) The method of claim 2, wherein the input data includes a
2 public key associated with the node.

1 4. (Original) The method of claim 2, wherein the input data includes a
2 static identifier associated with the node.

1 5. (Original) The method of claim 2, wherein an IPv6 address field of
2 the data packet is comprised of a 64-bit prefix followed by the most-significant 64
3 bits of the output of the non-reversible function, and wherein a universal/local bit
4 and an individual/group bit of the IPv6 address are both set to “0”.

1 6. (Original) The method of claim 5, wherein a SIP Call-ID field of
2 the data packet is comprised of a local-id and a host address, wherein
3 the local-id is comprised of the least-significant 128 bits of the output of
4 the non-reversible function; and wherein
5 the host address is comprised of the IPv6 address.

1 7. (Original) The method of claim 2, wherein an SSH public-key
2 fingerprint field of the data packet is comprised of the least-significant 128 bits of
3 the output of the non-reversible function.

1 8. (Original) The method of claim 2, wherein a MAC address field of
2 the data packet is comprised of the least-significant 64 bits of the output of the
3 non-reversible function.

1 9. (Original) The method of claim 2, wherein a JXTA Peer-ID field of
2 the data packet is comprised of the least-significant 128 bits of the output of the
3 non-reversible function.

1 10. (Original) The method of claim 2, wherein a JXTA Group-ID field
2 of the data packet is comprised of the least-significant 128 bits of the output of the
3 non-reversible function.

1 11. (Currently Amended) An apparatus for communicating
2 cryptographic data through multiple network layers, comprising:
3 a receiving mechanism configured to receive the cryptographic data at a
4 node;
5 a dividing mechanism configured to divide the cryptographic data into
6 multiple pieces; and
7 an encapsulation mechanism configured to simultaneously encapsulate
8 different pieces of the cryptographic data in fields associated with different
9 network layers of a protocol stack in a data packet, wherein the cryptographic data
10 is larger than a single field, and wherein the cryptographic data is encapsulated
11 within multiple fields associated with different network layers of the protocol
12 stack
13 wherein the multiple fields ~~need to be~~are received simultaneously by a
14 receiving node ~~to that~~ reconstructs an identity associated with the cryptographic
15 data; and
16 wherein the multiple fields ~~need to be~~are encapsulated simultaneously
17 into the data packet to ensure that the data packet can be routed through a network
18 to reach the receiving node.

1 12. (Original) The apparatus of claim 11, wherein the receiving
2 mechanism is configured to perform at least one non-reversible function on a
3 piece of input data to produce the cryptographic data.

1 13. (Original) The apparatus of claim 12, wherein the input data
2 includes a public key associated with the node.

1 14. (Original) The apparatus of claim 12, wherein the input data
2 includes a static identifier associated with the node.

1 15. (Original) The apparatus of claim 12, wherein an IPv6 address field
2 of the data packet is comprised of a 64-bit prefix followed by the most-significant
3 64 bits of the output of the non-reversible function, and wherein a universal/local
4 bit and an individual/group bit of the IPv6 address are both set to “0”.

1 16. (Original) The apparatus of claim 15, wherein a SIP Call-ID field
2 of the data packet is comprised of a local-id and a host address, wherein
3 the local-id is comprised of the least-significant 128 bits of the output of
4 the non-reversible function; and wherein
5 the host address is comprised of the IPv6 address.

1 17. (Original) The apparatus of claim 12, wherein an SSH public-key
2 fingerprint field of the data packet is comprised of the least-significant 128 bits of
3 the output of the non-reversible function.

1 18. (Original) The apparatus of claim 12, wherein a MAC address field
2 of the data packet is comprised of the least-significant 64 bits of the output of the
3 non-reversible function.

1 19. (Original) The apparatus of claim 12, wherein a JXTA Peer-ID
2 field of the data packet is comprised of the least-significant 128 bits of the output
3 of the non-reversible function.

1 20. (Original) The apparatus of claim 12, wherein a JXTA Group-ID
2 field of the data packet is comprised of the least-significant 128 bits of the output
3 of the non-reversible function.

1 21. (Currently Amended) A computer system for communicating
2 cryptographic data through multiple network layers, comprising:
3 a central processing unit;
4 a semiconductor memory;
5 a receiving mechanism configured to receive the cryptographic data at a
6 node;
7 a dividing mechanism configured to divide the cryptographic data into
8 multiple pieces; and
9 an encapsulation mechanism configured to simultaneously encapsulate
10 different pieces of the cryptographic data in fields associated with different
11 network layers of a protocol stack in a data packet, wherein the cryptographic data
12 is larger than a single field, and wherein the cryptographic data is encapsulated
13 within multiple fields associated with different network layers of the protocol
14 stack;
15 wherein the multiple fields ~~need to be~~are received simultaneously by a
16 receiving node ~~to that~~reconstructs an identity associated with the cryptographic
17 data; and
18 wherein the multiple fields ~~need to be~~are encapsulated simultaneously into
19 the data packet to ensure that the data packet can be routed through a network to
20 reach the receiving node.

1 22. (Original) The computer system of claim 21, wherein the receiving
2 mechanism is configured to perform at least one non-reversible function on a
3 piece of input data to produce the cryptographic data.

1 23. (Original) The computer system of claim 22, wherein the input data
2 includes a public key associated with the node.

1 24. (Original) The computer system of claim 22, wherein the input data
2 includes a static identifier associated with the node.

1 25. (Original) The computer system of claim 22, wherein an IPv6
2 address field of the data packet is comprised of a 64-bit prefix followed by the
3 most-significant 64 bits of the output of the non-reversible function, and wherein
4 a universal/local bit and an individual/group bit of the IPv6 address are both set to
5 “0”.

1 26. (Original) The computer system of claim 25, wherein a SIP Call-ID
2 field of the data packet is comprised of a local-id and a host address, wherein
3 the local-id is comprised of the least-significant 128 bits of the output of
4 the non-reversible function; and wherein
5 the host address is comprised of the IPv6 address.

1 27. (Original) The computer system of claim 22, wherein an SSH
2 public-key fingerprint field of the data packet is comprised of the least-significant
3 128 bits of the output of the non-reversible function.

1 28. (Original) The computer system of claim 22, wherein a MAC
2 address field of the data packet is comprised of the least-significant 64 bits of the
3 output of the non-reversible function.

1 29. (Original) The computer system of claim 22, wherein a JXTA
2 Peer-ID field of the data packet is comprised of the least-significant 128 bits of
3 the output of the non-reversible function.

1 30. (Original) The computer system of claim 22, wherein a JXTA
2 Group-ID field of the data packet is comprised of the least-significant 128 bits of
3 the output of the non-reversible function.

1 31. (Currently Amended) A method for verifying a data packet
2 containing cryptographic data, comprising:
3 receiving the data packet;
4 extracting pieces of cryptographic data from fields associated with
5 different network layers of a protocol stack within the data packet, wherein the
6 cryptographic data is larger than a single field, and wherein the cryptographic data
7 is simultaneously encapsulated within multiple fields; and
8 verifying that each piece of extracted cryptographic data matches with a
9 corresponding portion of a piece of previously obtained cryptographic data;
10 wherein the multiple fields ~~need to be~~are received simultaneously to
11 reconstruct an identity associated with the cryptographic data; and
12 wherein the multiple fields ~~need to be~~are simultaneously encapsulated into
13 the data packet by a sending node to ensure that the data packet can be routed
14 through a network to reach a receiving node.

1 32. (Original) The method of claim 31, wherein the previously
2 obtained cryptographic data is obtained through a process that involves
3 performing at least one non-reversible function on a piece of input data to produce
4 the cryptographic data.

1 33. (Previously Amended) An apparatus for verifying a data packet
2 containing cryptographic data, comprising:
3 a receiving mechanism configured to receive the data packet;
4 an extracting mechanism configured to extract pieces of cryptographic
5 data from fields associated with different network layers of a protocol stack within
6 the data packet, wherein the cryptographic data is larger than a single field, and
7 wherein the cryptographic data is simultaneously encapsulated within multiple
8 fields; and

9 a verification mechanism configured to verify that each piece of extracted
10 cryptographic data matches with a corresponding portion of a piece of previously
11 obtained cryptographic data.

1 34. (Original) The apparatus of claim 33, wherein the previously
2 obtained cryptographic data is obtained through a process that involves
3 performing at least one non-reversible function on a piece of input data to produce
4 the cryptographic data.

1 35. (Currently Amended) A computer system for verifying a data
2 packet containing cryptographic data, comprising:
3 a central processing unit;
4 a semiconductor memory;
5 a receiving mechanism configured to receive the data packet;
6 an extracting mechanism configured to extract pieces of cryptographic
7 data from fields associated with different network layers of a protocol stack within
8 the data packet, wherein the cryptographic data is larger than a single field, and
9 wherein the cryptographic data is simultaneously encapsulated within multiple
10 fields; and
11 a verification mechanism configured to confirm that each piece of
12 extracted cryptographic data matches with a corresponding portion of a piece of
13 previously obtained cryptographic data;
14 wherein the multiple fields ~~need to be~~are received simultaneously to
15 reconstruct an identity associated with the cryptographic data; and
16 wherein the multiple fields ~~need to be~~are simultaneously encapsulated into
17 the data packet by a sending node to ensure that the data packet can be routed
18 through a network to reach the receiving mechanism.

1 36. (Original) The computer system of claim 35, wherein the
2 previously obtained cryptographic data is obtained through a process that involves
3 performing at least one non-reversible function on a piece of input data to produce
4 the cryptographic data.